

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

LYNNE FREEMAN,

Plaintiff,

v.

TRACY DEEBE-ELKENANEY P/K/A
TRACY WOLFF, et al.,

Defendants.

Case No.: 1:22-cv-02435-LLS-SN

DECLARATION OF BENJAMIN ROSE

Benjamin Rose declares as follows:

1. I am the President of Carden Rose, Inc., a digital investigations and electronic discovery consulting firm. I am also a licensed private investigator in the State of California. This declaration is based on my own personal knowledge, except where indicated, and as to those matters if I am called as a witness, I could and would testify competently thereto. As to those matters stated on information and belief, I am informed and believe them to be true.

2. As President of Carden Rose, Inc., I am familiar with how data are stored on various digital media devices and have conducted approximately one thousand (1,000) forensic investigations of digital evidence over the past seventeen (17) years. I have managed, collected, preserved, processed, and produced digital evidence in thousands of legal matters.

3. During my career, I have testified as an expert witness in various Superior Courts within the State of California. I have also provided written testimony in a number of legal matters at both the State and Federal levels. Some of these occurrences are included in my Curriculum Vitae, which is attached hereto as **Exhibit A**.

4. I was retained by Cowan DeBaets Abrahams & Sheppard LLP to collect, search, and produce Electronically Stored Information (“ESI”) for Counsel’s review in the matter listed above. I am informed by Counsel that Plaintiff has alleged improper conduct related to discovery. Specifically, I reviewed Plaintiff’s letter to the Court, dated February 22, 2023, requesting a Motion to Compel Inspection of a Defendant’s computer hard drives and to gain access to their email account. I am troubled by Plaintiff’s assertions, which I will describe in detail below.

5. Plaintiff referenced two (2) emails with attached word documents from the email account mel1542@sbcglobal.net, which belongs to Defendant Tracy Wolff. I collected the emails from that account with Metaspike’s Forensic Email Collector¹, by logging into the email account using the correct login credentials that Ms. Wolff supplied. During the collection process, no alteration or manipulation of any email occurred.

6. I processed the email account in Vound Software’s Intella, an email investigation and eDiscovery software tool. I exported potentially responsive emails and attachments for Counsel’s review, as part of my post-collection tasks. No alteration or manipulation of data occurred at this stage of the eDiscovery process. I uploaded the data to Counsel’s document review tool; no manipulation of data occurred at this stage either.

7. Plaintiff believes the email and attachments in question were backdated, and further alleges a second email that Ms. Wolff sent to one of her other email accounts was backdated as well. Plaintiff stated a computer forensics expert examined the above-described emails and attachments, and concluded they are suspicious, though the individual has not been identified.

¹ Forensic Email Collector is a desktop application used for forensic collection and preservation of electronic mailboxes, directly from email servers. The software program authenticates the collection of email, thus maintaining the integrity of the data.

8. I am informed Defendant produced documents and emails in Adobe Portable Document Format (PDF), and subsequently produced these particular emails in native file format. Plaintiff asserts the emails are questionable as they did not contain a Message-ID.² I examined the emails in question and a sampling of other sent emails from Ms. Wolff's mailbox; no emails in the Sent folder contained a Message-ID. This characteristic itself is not evidence of fraud or manipulation. The result could be based upon the account configuration settings, including the mail protocol that was used in 2010, when the messages were sent. Due to the lapse in time from 2010, there is no reasonable way to validate what those settings consisted of on Ms. Wolff's account.

9. I exported the Emails Header Reports, which are attached as **Exhibit B**. The reports reveal the date and timestamp of the emails, the Internet Protocol ("IP") address, the email domain Yahoo³, and the source of the mail client "HTTP."⁴ I also examined a hidden date and time stamp, contained in the Content-Type field. The values were 1282760135 and 1284778676. I used Digital Detective's D-Code program to convert the date and time in Unix Seconds,⁵ which indicated the dates and times of 08/25/2010 11:15:35.0000000 -07:00 and 09/17/2010 19:57:56.0000000 -07:00.⁶

10. I compared the email header information in my personal SBCGlobal.net account⁷ at or around the same dates as Wolff's emails in question and found the included fields to be

² A Message-ID is a unique identifier that may be contained in email message headers.

³ SBCGlobal.net email addresses use Yahoo's email service.

⁴ Hyper Text Transfer Protocol is the technical name for a Webpage; in this case, it reveals a Web Browser was used to send the email in question.

⁵ Unix Seconds or Unix Epoch is the number of seconds since January 1, 1970. It is a standard used in the technology industry.

⁶ -07:00 is minus seven (7) hours from Universal Time Coordinated (UTC), which is a global time standard. The date and time are consistent with the email header information on both emails, as the email collection was configured in Pacific Standard Time.

⁷ Personal identifiers have been removed for privacy.

consistent with those in Wolff's email account. They also included a source IP address, email domain, Web Browser indicator and date and timestamp, including the hidden date and time in the Content-Length field. These emails also did not contain a Message-ID. The reports are attached as **Exhibit C**.

11. Plaintiff contends the August 25, 2010 email attachment, identified as a Microsoft Word document named "tempest rising" was either backdated or manipulated. I conducted a forensic review of the file in Intella, which revealed the following metadata: The document was created in Microsoft Word (97-2003) on June 30, 2010 7:12:00 AM PDT, it was approximately 851 Kilobytes (KB). The Content Last Modified date and time stamp was also on June 30, 2010 7:12:00 AM PDT. The Creator field and all saved versions⁸ were identified as "Author."⁹ The word count was approximately 90,000; no page count was listed. I printed the file properties report, which is attached as **Exhibit D**.

12. An additional Microsoft Word document named "tempest rising" was located with a creation date and time of March 4, 2011 at 8:19:00 PM PST. The size was approximately 722 KB. The Content Last Modified date and time stamp was on March 4, 2011 at 8:20:00 PM PST. Although the word count was approximately 70,000 on a Windows computer, a review of the metadata on an Apple computer revealed approximately 90,000 words. I believe the metadata on the Apple computer is more reliable and the count on a Windows computer is incorrect and may be an anomaly. I took a screenshot of the metadata and have attached it as **Exhibit E**. I viewed both documents in their native application (Microsoft Word) and found both files to be 451 pages in a side-by-side page view. I believe Plaintiff's analysis was

⁸ Microsoft maintains hidden information about the last ten (10) authors who edited a document. These data are not visible to the user of the program.

⁹ The identification of a document creator is optional and may be selected upon installation of the Microsoft Word program or modified per document.

incorrect. I didn't observe any other evidence of irregularities and do not believe this proves any alteration of the documents.

13. Plaintiff further alleges "unusual" metadata suggests manipulation, including the "author" name of the documents. The reference is the use of the names "owner," "Author," "tracy" and "tracy elkenaney." Plaintiff further opines Custodian usernames such as "tracy" or "tracy elkenaney" would be considered standard user accounts. Plaintiff alleges "Author" and "owner" are non-standard, suggesting possible masking or manipulation of metadata in the Word documents. This is incorrect; author names are optional and selective, based upon the Microsoft Word user's desire for identification. There are no mandated standards for this selection and Plaintiff uses the terms "user accounts" and "usernames" interchangeably, which is also in error. There are no known "non-standard" author names, the user's decision is completely arbitrary.

14. The assertion of approximately 1062 Word documents produced, where only two (2) Word documents contained the username "Author" is neither suspicious nor evidence of wrongdoing. I reviewed the documents in the email file and identified the following instances of usernames: "owner" (62), "Owner" (8), "Author" (3), "tracy" (9), "Tracy Deebs-Elkenaney" (9), "tracy elkenaney" (1), "user" (2), "User" (1), "Admin" (5), and "Administrator" (5). I did not find any pattern related to the choice of usernames on the documents, nor did I verify each document to determine if they were created by the Defendant or received as an attachment to an email. The results are to demonstrate there are no "standard" or "non-standard" usernames.


15. Plaintiff assumes "at least three different computers were used to create most of these files. At least two computers can be identified within all of the seven files." I do not find any evidence from the emails or documents to support this statement. In fact, a computer may

be identified as the source of creation or storage of a document; documents do not identify computers as the source of their creation.

16. I disagree Plaintiff is “entitled” to inspect Defendant’s computer hard drives and email account. In my experience, this is not a case that justifies a forensic examination of Defendant’s computers and email account. Standard eDiscovery processes and tools have been employed for the identification, collection, preservation, and searches of ESI have been employed, which has resulted in the identification of potentially responsive material and while maintaining the ability to protect the Defendant’s privacy, as well as exclude non-responsive items. In my opinion, allowing Plaintiff to create mirror images of Defendant’s hard drives, based on suspicions, is intrusive and excessive, and is not proportional or warranted based on Plaintiff’s assertions.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: March 3, 2023



Benjamin Rose